08/15/01

05-16-01 JC20 Rec'd PCT/PTO 15 AUG 2001

FORM PTO-1390 (Modified) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE
(REV 11-2000)

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
537-1052	
U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5)	
09/913785	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/GB00/00447	February 11, 2000	February 19, 1999

TITLE OF INVENTION

Data Encoding/Decoding Device and Apparatus Using the Same

APPLICANT(S) FOR DO/EO/US

Clive Jones and Richard Hollingshead

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
 a. ☐ is attached hereto (required only if not communicated by the International Bureau).
 b. ☒ has been communicated by the International Bureau.
 c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
 a. ☐ is attached hereto.
 b. ☐ has been previously submitted under 35 U S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
 a. ☒ are attached hereto (required only if not communicated by the International Bureau).
 b. ☒ have been communicated by the International Bureau.
 c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A copy of the International Search Report (PCT/ISA/210)

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☐ Other items or information:

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/913785	PCT/GB00/00447	537-1052

531 Rec'd PCT/PTO 15 AUG 2001

24. The following fees are submitted:.		CALCULATIONS PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1000.00**	
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	**$860.00**	
☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**	
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**	
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =		**$860.00**
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		**$0.00**

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	18 - 20 =	0	x $18.00	**$0.00**	
Independent claims	6 - 3 =	3	x $80.00	**$240.00**	
Multiple Dependent Claims **(check if applicable)**			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$1,100.00**	
☐ Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$1,100.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE =				**$1,100.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				**$0.00**	
TOTAL FEES ENCLOSED =				**$1,100.00**	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of $1,100 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 12-0913 A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Lee, Mann, Smith, McWilliams, Sweeney and Ohlson
209 S. La Salle
Suite 410
Chicago, IL 60604

William M. Lee

SIGNATURE

William M. Lee, Jr.

NAME

26,935

REGISTRATION NUMBER

August 15, 2001

DATE

09/913785
531 Rec'd PCT 15 AUG 2001

Docket No.: 537-1052

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE THE APPLICATION OF:)
)
Clive Jones and Richard Hollingshead)
)
SERIAL NO. To Be Assigned Herewith)
)
FILING DATE: Herewith)
)
FOR: Data Encoding/Decoding Device)
and Apparatus Using the Same)
)

AMENDMENT ACCOMPANYING APPLICATION

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231-9998

Dear Sir:

The present application is the National Filing of International Application No. PCT/GB00/00447. Appended hereto is a copy of the International Preliminary Examination Report for that application. Before calculation of the National Filing Fee for the United States, it is requested that the application be amended as follows:

IN THE CLAIMS

Amend claims 6-8, 11, 13, 15, and 18 as follows:

6. (Amended) A data encoding device as claimed in claim 1, wherein the combination performed by the encoding unit is carried out more rapidly than the time associated with the reception of each input bit from the serial data input, such that the encoded output bit represents the input bit with zero delay.

7. (Amended) A data encoding device as claimed in claim 1, wherein the input comprises digital audio data.

8. (Amended) An apparatus for generating digital audio data comprising:

a source of digital audio signals;

a data encoding device having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and a plurality of updated encoding bits, wherein each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein the combination function performed by the encoding unit combines the input bit with a function of the key, such that over time the encoded output bit stream comprises substantially white noise; and a transmitter for supplying the encoded serial data output to an output port of the apparatus.

11. (Amended) A data decoding device for decoding a serial data stream encoded by an encoding device, wherein the stream of input bits is supplied to a decoding unit which combines each encoded input bit with a plurality of additional decoding bits, to extract a decoded output bit and an updated plurality of decoding bits.

13. (Amended) An apparatus for reconstructing digital audio signals comprising an input for receiving encoded digital audio signals, a receiver for supplying the encoded digital audio signals to a decoding device, and an output for the reconstructed digital audio signal.

15. (Amended) A data communications system comprising:

an apparatus for generating digital audio data including: a source of digital audio signals; a data encoding device having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and a plurality of additional encoding bits, wherein each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein the combination function performed by the encoding unit combines the input bit with a function of the key, such that over time the encoded output bit stream comprises substantially white noise; and a transmitter for supplying the encoded serail data output to an output port of the apparatus, for providing an encoded digital audio output, and

an apparatus for reconstructing digital audio signals comprising an input for receiving encoded digital audio signals, a receiver for supplying the encoded digital audio signals to a decoding device, and an output for the reconstructed digital audio signal.

18. (Amended) An apparatus as claimed in claim 16, wherein the format having a separate clock channel comprises the I^2C data format.

REMARKS

The above amendments are being made in order to eliminate multiple dependency and improper multiple dependency before calculation of the filing fee for the United States. Should any multiple dependency remain, that is unintended, and the Patent and Trademark Office is requested to cancel any remaining multiple dependent claims without prejudice before calculation of the application filing fee.

Examination of the application on its merits is awaited.

Respectfully submitted,

Date: August 15, 2001

William M. Lee, Jr.
Registration No. 26, 935

Lee, Mann, Smith, McWilliams,
Sweeney & Ohlson
P. O. Box 2786
Chicago, Illinois 60690-2786
312-368-6620 Direct Line
312-368-1300 Telephone
312-368-0034 Facsimile
wlee@intelpro.com Email

09/935,826

531 Rec'd PCT/PTO 15 AUG 2001

VERSION WITH MARKINGS TO SHOW CHANGES MADE

6. (Amended) A data encoding device as claimed in claim [any preceding claim] 1, wherein the combination performed by the encoding unit is carried out more rapidly than the time associated with the reception of each input bit from the serial data input, such that the encoded output bit represents the input bit with zero delay.

7. (Amended) A data encoding device as claimed in [any preceding] claim 1, wherein the input comprises digital audio data.

8. (Amended) An apparatus for generating digital audio data comprising:

a source of digital audio signals;

a data encoding device [as claimed in any preceding claim] having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and a plurality of updated encoding bits, wherein each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein the combination function performed by the encoding unit combines the input bit with a function of the key, such that over time the encoded output bit stream comprises substantially white noise; and a transmitter for supplying the encoded serial data output to an output port of the apparatus.

11. (Amended) A data decoding device for decoding a serial data stream encoded by an encoding device [of any one of claims 1 to 7], wherein the stream of input bits is supplied to a decoding unit which combines each encoded input bit with a plurality of additional decoding bits, to extract a decoded output bit and an updated plurality of decoding bits.

13. (Amended) An apparatus for reconstructing digital audio signals comprising an input for receiving encoded digital audio signals, a receiver for supplying the encoded digital audio signals to a decoding device [as claimed in claim 11 or 12], and an output for the reconstructed digital audio signal.

15. (Amended) A data communications system comprising:

an apparatus [as claimed in claim 8,9 or 10] for generating digital audio data including: a source of digital audio signals; a data encoding device having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and a plurality of additional encoding bits, wherein each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein the combination function performed by the encoding unit combines the input bit with a function of the key, such that over time the encoded output bit stream comprises substantially white noise; and a transmitter for supplying the encoded serail data output to an output port of the apparatus, for providing an encoded digital audio output, and

an apparatus [as claimed in claim 13 or 14] for reconstructing digital audio signals comprising an input for receiving encoded digital audio signals, a receiver for supplying the encoded digital audio signals to a decoding device, and an output for the reconstructed digital audio signal.

18. (Amended) An apparatus as claimed in claim 16 [or 17], wherein the format having a separate clock channel comprises the I^2C data format.

DATA ENCODING/DECODING DEVICE AND APPARATUS USING THE SAME

This invention relates to data encoding and decoding devices, particularly for serial digital data. This data may in one particular example be for transmission between different parts of an audio data processing system.

Currently, the output of audio or video reproduction equipment comprises a collection of data, formatted in accordance with the prescribed interface protocol. There is, however, a desire for digital output signals from such equipment to be encoded so that these output signals cannot be digitally recorded, for example to duplicate information stored on a CD or CD-ROM. This invention is concerned with the encoding of data particularly at the interfaces between audio or video data processing equipment.

This invention is applicable to digital serial data, irrespective of the original signal represented by the digital data. However, a further problem arises specifically in connection with digital audio data and the particular data formats currently used for transmitting such data between audio equipment.

Two similar standards have achieved widespread recognition and use for the encoding of digital audio data - the Sony Philips Data Interface Format ("SPDIF") and the Audio Engineering Society/European Broadcasting Union format ("AES/EBU"). The SPDIF format is most often used in products directed to the consumer market, whereas the AES/EBU format is most often used in equipment for professional applications.

Both of these standards use a biphase-mark encoded data stream to transmit digital audio information in serial format. In this biphase-mark encoding, each bit of data always starts with a transition of the signal and ends with a transition of the signal. If a transition occurs in the middle of the period, a one is encoded, otherwise a zero is encoded.

The use of biphase-mark encoding has several well-known advantages, the most important of which for this application is that biphase-mark encoding is self-clocking. Thus, as every bit starts and ends with a transition, the biphase-mark encoded data can be used to generate

or recover a clock signal for use with the data. Therefore, apparatus receiving the encoded data in SPDIF or AES/EBU format does not require a local clock, but can instead derive the clock signal from the received encoded data.

A problem with the reconstruction of a clock signal from a received encoded input is that digital to analogue converters used in audio equipment require spectrally pure clock signals in order to operate satisfactorily at high resolution. The purity of the clock signal derived from the encoded data is worsened by the transmission of the data signal, for example over a coaxial cable. However, the effect of this transmission on the clock signal is reduced if the encoded data carrying the clock signal has a flat frequency spectrum.

According to the present invention there is provided a data encoding device having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits, to derive an encoded output bit and a plurality of updated encoding bits, the function performed by the encoding unit being selected such that over time the encoded output bit stream comprises substantially white noise.

Thus, the invention provides an encoding device in which the encoding unit is arranged to provide additional bits which operate on the input data to provide an output having constant and flat frequency response. Thus, the output of the encoding device is merely noise in the absence of an appropriate decoding device. Furthermore, the transmission of noise as the output of the encoding device enables a clock signal which is to be recovered from the data signal to be transmitted with minimum deterioration. This applies regardless of the type of data being transmitted, but for audio data the recovery of a spectrally pure clock signal is particularly desirable.

The additional encoding bits may initially be derived from a random number generator to enable initialisation of the encoding device. The introduction of a random element increases the entropy of the encoding device.

It is of course necessary for information concerning the random element used in the encoding

operation to be transmitted with the encoded data to enable subsequent decoding. A problem then arises that this information occupies bandwidth of the transmission channel. A large number of encoding bits is desired to improve the security of the encryption, whereas it may only be possible to provide a small number of bits relating to the random number in the available bandwidth of the transmission channel allocated to this type of control data.

This random number is preferably therefore encoded internally using a transformation unit which expands the random number. Preferably, the serial input comprises a string of digital words each comprising a predetermined number of bits, and wherein the random number generator is clocked using a word clock, such that for each digital word of the input a new random number bit is generated. The transformation unit then comprises means for storing a predetermined number of previous values of the one bit random number to derive a multiple bit random word.

A permutation unit is preferably provided to operate on the multiple bit random word, to generate as output the additional encoding bits, the permutation unit having a function such that the latching operation of the transformation unit cannot be derived from the additional encoding bits.

The random number is preferably encoded using a further transformation unit, with the transformed random number being provided as an output of the data encoding device. This enables the transformed random number to be provided to an associated decoding device to enable reconstruction of the original data.

The encoding unit is preferably re-initialized by output of the permutation unit once for each word. This arrangement enables the encoding device to re-initialize itself after each word. For audio applications, a word typically comprises two data samples, one for each stereo output. This arrangement enables a system having an encoding device and a decoding device to regain communication with minimum of delay in the event of a failed transmission between the two devices. Also, the encryption or scrambling performed by the encoding device may be turned on or off with minimum disruption.

The encoding device preferably is arranged such that the encoded output bit represents the input bit with zero bit delay.

The invention also provides an apparatus for generating digital audio data comprising a source of digital audio signals, a data encoding device of the invention and a transmitter for supplying the encoded serial data output to an output port of the apparatus. This apparatus may comprise a compact disc player. The serial data output preferably comprises digital audio data which may be arranged in the SPDIF or AES/EBU format.

The invention also provides a data decoding device for decoding a serial data stream encoded by an encoding device of the invention. This decoding device may be used in an apparatus for reconstructing digital audio signals, such as a speaker.

According to a second aspect of the invention, there is provided an apparatus for encoding digital audio signals, the apparatus having an audio input in a format having a dedicated clock signal channel and an encoded audio output in a format having an intrinsically defined clock signal in the output data stream, wherein the audio input is encoded such that the encoded audio output comprises substantially white noise, and the output of the apparatus additionally comprises control data for enabling the audio input to be reconstructed at an associated decoding device.

This apparatus can increase the security of data transmission, whilst additionally providing the advantage of improved recovery of the clock signal which is recovered from the encoded signal.

The output format having an intrinsically defined clock signal may use biphase-marking, for example the SPDIF or AES/EBU data format. In this case, the control data may be carried on (at least) the U channel. This is particularly desirable, since conventional recording equipment operating according to these formats does not record the U channel, so that the security of the encryption is enhanced. The format having a separate clock channel may comprise the I^2C data format.

The invention will now be described by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows a conventional serial data transmission;

Figure 2 shows the frame structure of SPDIF or AES/EBU data and the structure of individual sub-frames;

Figure 3 shows a data transmission system using decoding and encoding in accordance with the invention;

Figure 4 shows in greater detail an encoding unit of the invention and

Figure 5 shows in greater detail a decoding unit of the invention.

A conventional data transmission system, for transferring data between data processing apparatus is shown in Figure 1. As an example, the transmitting apparatus Tx of Figure 1 may be within a compact disc player, and the receiving apparatus Rx may be within a loud speaker. In this case, the data to be transferred comprises audio data, and the specific example described below is an audio application of the invention, although the invention is not limited to audio data.

In order to control the transmission of data, the transmission circuit Tx is provided with control data as well as the data to be transmitted, and additionally a clock signal CLK which provides the timing information.

Two similar standards are now widespread for the encoding of digital audio data, the Sony Philips Data Interface Format ("SPDIF") and the Audio Engineering Society/European Broadcasting Union standard ("AES/EBU"). These standards both use a biphase-mark encoded data stream to transmit digital audio information in serial format. This biphase-mark encoding is well known in the art and will not be described in detail. However, it is worthy of note that this encoding technique is self-clocking, so that the clock signal which governs the control of the transmission circuit is effectively recoverable by the receiver from the encoded data stream itself, so that the receiver does not need an independent synchronized clock.

The SPDIF and AES/EBU standards also define the manner in which data is defined into

frames and sub-frames. Figure 2 shows the frame format used in the SPDIF and AES/EBU standards. Within each frame F_0, F_1, F_2 ... , two channels of audio data are transmitted, namely channels A and B, ChA, ChB. The beginning of each channel A and B is identified by the preambles X and Y, respectively.

A frame comprises a single sample of the audio data for channel A and channel B, together with associated preambles X and Y and any auxiliary data or non-audio data bits. Each frame F thus comprises two sub-frames, one for each channel. One such sub-frame is shown in Figure 2 in expanded form, and comprises the audio data AUDIO for the respective channel, together with the associated preamble PREAMB and any auxiliary data AUX and additional non-audio data bits V, U, C, P. Thus, as shown in Figure 2, bit positions b_0 to b_{31} make up the sub-frame. The preamble PREAMB occupies bit positions b_0 to b_3, and auxiliary data AUX which occupies bit positions b_4 to b_7 may either provide non-audio information or may be used as part of the audio data. This audio data occupies bit positions b_8 to b_{27}, and together with the available auxiliary data a 24 bit sample for each channel may be provided. Four additional bits of non-audio data are also included comprising a validity bit V, to indicate whether the data within the sub-frame is suitable for conversion to analogue, a user data bit U which can be used for any purpose, a channel status bit C and a parity bit P.

As will be known to those skilled in the art, the preambles X, Y may each begin with a digital pulse that is 1.5 times the sample time in duration. This is a violation of the biphase-mark encoding rule that each cell is bordered by a transition. Thus, each preamble begins with a code violation to distinguish the preamble from any other event in the data stream.

To the extent described above, the SPDIF and AES/EBU standards are identical. The difference between these two standards is that the use of the user data and channel status data bits differ.

As described above, biphase-mark encoding provides a self-clocking digital signal. Conventionally, a phase-locked loop is used to recover a clock signal from the data signal transmitted. In such a device, a digital edge-triggered phase detector is coupled to a voltage-

controlled oscillator. Through a feedback loop, the VCO is used to generate an independent clock signal having a frequency design to match the clocking of the incoming biphase-mark encoded signal. Alternatively, a clock signal may be based on the amount of time that passes between the preamble signals, although in the encoding scheme of this invention a clock cycling at the transmission rate of individual bits is required, as will be described in the following.

There is increasingly a desire to provide a level of security for the data transmitted between different equipment within a data processing system. For example, in the conventional data transmission system represented in Figure 1, the data 10 transmitted over the serial coaxial cable may simply be recorded with digital recording equipment so that copies of the original data source may be generated. To prevent unauthorized copying, there is a requirement for data transmitted between different pieces of equipment (for example compact disc players and speakers) to be provided in encoded format.

Furthermore, a problem with the use of a self-clocking digital interface is that the recovered clock will exhibit "jitter" correlated to the data on the interface. In many applications, the accuracy and spectral purity of the clock that can be recovered by the receiver Rx is important, and the recovery of the clock will be more accurate the more closely the data on the interface approximates a random bit stream.

Figure 3 shows in schematic form an encoding technique according to the invention, in which an encoder 20 is interposed between the original data source and the transmitter Tx, and a decoder 50 is interposed between the transmitter Rx and the output. The encoder and decoder still enable the conventional standardized transmitter Tx and receiver Rx to be utilized, for example which may operate according to the SPDIF or AES/EBU format. In accordance with the invention, the effect of the encoder 20 is to encode at least the audio data from the input so that the encoded output D′ comprises substantially white noise, and wherein encoded control data C′ is provided to enable the audio input data to be reconstructed at the decoding device 50. By providing an encoding scheme which gives a data output D′ comprising substantially white noise, the recovery of the clock signal is greatly improved which particularly assists in subsequent digital to analogue conversion.

Furthermore, the security of the transmission is also improved.

The functions performed by the encoding device 20 and the decoding device 50 may be standardized for all equipment, so that the relationship between the data 10 and the input data is known. However, it is preferred that the conversion of the data also effects scrambling of the data, so that the exact construction of the encoder 20 and decoder 50 are kept secret and must be known in order to derive any useful information from the data 10. In this case, the functions of clock recovery improvement and of data scrambling are combined, so that these functions may be performed in a single piece of apparatus. A preferred scrambling technique according to the invention will now be described in greater detail.

Figure 4 shows an apparatus 18 for generating encoded data DATA′ which includes an encoder 20 as represented schematically in Figure 3.

The encoder 20 receives a digital signal from a data source 22, for example a compact disc reader for audio or video data. The data from the data source 22 is provided to an encoding unit 24 which provides the encoded data DATA′. The data from source 22 can include the conventional control data so that the output data DATA' includes part of the encoded control data C' shown in Figure 3.

The encoding unit 24 receives the input data as a serial data bit stream 25 and which is provided to a combinatorial unit 26. This unit 26 combines each input bit from the bit stream 25 with an additional number α of encoding bits 27 so as to generate an encoded data output bit 28 and an updated set 27′ of the α encoding bits. These updated encoding bits 27′ are supplied by a feedback path through a latch mechanism (not shown) to a multiplexer 30. The multiplexer 30 normally passes these updated encoding bits 27′ to the combinatorial unit 26 for processing of the subsequent bit of the data bit stream 25. The operation of the multiplexer 30 will be described in greater detail in the following.

The purpose of the combinatorial unit 26 is to provide an output data bit stream DATA′ which has the spectral response of substantially white noise, namely a substantially flat spectral response over the frequency range of interest. To achieve this, the input data from

the bit stream 25 may be combined with a known function of the encoding bits 27 using an XOR function. Thus:

$$DATA' = DATA \oplus f(EB),$$ where EB are the encoding bits 27.

This function may be implemented simply as a look-up table, which also provides the updated encoding bits 27′ as a function of the data input and the current encoding bits. Thus:

$$EB' = g(DATA, EB),$$ where EB′ are the updated encoding bits 27′.

The updating of the encoding bits is carried out once for each new bit from the input bit stream 25, so that the encoding unit 24 requires a bit clock signal BCLK which is shown only schematically in Figure 4 as being supplied to the unit 24. The exact arrangement of latching and sequencing elements required in the encoding unit 24 will not be described, since these will be apparent to those skilled in the art.

The operation of the encoding unit is therefore essentially to encrypt each input bit with a string of bits forming an encryption key, and wherein each subsequent input bit is encrypted using a modified key which is derived from previous values of the key and of the input bit.

The design of the encoding unit 24 described above enables the encoded output data to have the properties of white noise, but the data structure is preserved, so that conventional standardized interface protocols may be employed. Furthermore, the feedback of encoding bits described can enable the encoded output data DATA′ to be generated with 0 bit delay since the look-up table or other functional unit which constitutes the combinatorial unit 26 may be addressed in a shorter time period than the time associated with the reception of each individual bit from the data bit stream 25.

The zero bit delay of the encoding unit 24 enables the encryption to be switched on and off if desired, with minimum of delay.

When the operation of the apparatus 18 is started, there will be no updated encoding bits 27' to enable the encoding unit 24 to operate in a predictable manner. Consequently, a set of encoding bits must be provided for initialization of the encoder 20. An encoded random number is employed for this purpose. Thus, the apparatus 18 includes a random number generator 32 which provides a random or quasi-random output bit stream. As one example, the random number generator comprises a pseudo-random number generator with a cycle of many thousand iterations, and a source of unpredictable (but not white) data. These may be combined to give a white and unpredictable data source. The source of unpredictable data may be derived from data in another device of the apparatus (for example a microcontroller) performing unrelated functions, and preferably with different clocking, or may be derived from some other unrelated parameter. The pseudo-random number generator may comprise part of the encoder 20 (although this is not shown) so that the output can not be easily obtained.

The initialisation encoding bits must be conveyed to a decoding device of the system to which the encoded information is transmitted. However, the bandwidth available for the transmission of this type of control data may not be sufficient to provide an appropriate number of bits for the encoding unit 24. For example, in the case of SPDIF the signal derived from the random bit stream may be provided on the U channel of the data structure (as explained in the following), which provides only one bit per channel sample, as shown in Figure 2.

For this reason, a new random (or quasi-random) bit is generated only once for each input word. The random or quasi random output bit stream is supplied to a transformation unit 34 comprising a serial array of latches 36 which effectively store a number of bits from the previous history of the random number generator 32, so that a larger random word, suitable for generating the initialisation encoding bits, may be generated.

The array of latches comprises a number β of latches 36, and these latches are triggered with a sample clock signal SCLK. For example, if the data to be encoded comprises two 24 bit words of digital audio data, the sample clock SCLK will have a frequency 48 times lower than the bit clock BCLK. A new random number is therefore stored in the array of latches

36 for each digital word, although all but one of the bits of the random word will be in common with the previous random word.

In order to disguise the dependence of each random word on the previous random words, a permutation function may be performed on the random word (having β bits) in a permutation unit 38, which provides an output having a number α of bits corresponding to the required number of encoding bits in the encoding unit 24. The relationship between the output 40 and the history of the random number generator is thus not obvious to a third party. This output 40 is supplied to the encoding unit 24 as shown in Figure 4.

In a preferred example, at the beginning of each word of the input, the output 40 of the transformation unit is used to provide the first set of encoding bits 27 within the encoding unit 24. Subsequently, the feedback loop generates the updated encoding bits 27' for the subsequent encoding operation.

If the number α of initialisation bits is sufficiently large, the re-keying of the encoding scheme every word ensures that the function of the combinatorial unit 26 can not be determined by any simple inspection, as explained below.

The unit 26 has 2^{α} internal states, so that a full interrogation of the effect of each internal state could be determined by studying the output of the unit 26 for 2^{α} cycles, once for a constant input 25 of 1 and once for a constant input 25 of 0. Therefore, the number α of encoding bits is preferably selected such that $2^{\alpha+1}$ is greater than the number of bits in each word, so that the encoding unit 24 is re-keyed before a full interrogation can be performed. To provide the suitable number of encoding bits, the latch arrangement in the unit 34 is required, effectively to expand the random bit stream by storing previous values.

The arrangement described enables reception to be recovered after an interruption in the data signal with a maximum delay of one word. If the transmission of control data is interrupted, the correct control information for resumption of the transmission can be obtained after β words, since this enables the data in the full latch arrangement 34 to have been transmitted subsequently to the interruption.

To decode the encoded data stream, the function of the encoding unit 24 must be reversed, and additionally the initial encoding bits 27 used by the encoding unit 24 must be known. For this purpose, the random number produced by the random number generator 32 is also provided as an output of the apparatus 18, although this random series of bits is also provided through a transformation unit 42 to provide additional security. In a preferred example in which the data comprises digital audio data, and in which the output of the apparatus 18 is to be converted into in SPDIF or AES/EBU format, the encoded data DATA' may occupy the auxiliary and audio segments of each channel, as represented in Figure 2, whereas the transformed random number (i.e. the control data indicated in Figure 4) may occupy the U channel also represented in Figure 2, and optionally one or more other non-audio bits. For audio data to be formatted in accordance with these standards, this arrangement is preferred, as conventional digital audio recording equipment having an input in standardized SPDIF or AES/EBU format does not record the non-audio channels within the frame structure. Also, any corruption of the U channel (or other chosen channel), for example incorrect synchronisation, will prevent correct decoding.

An optional additional function performed by the encoding unit 20 is to set the validity bit V to a value which indicates that D/A conversion of the data conveyed is not appropriate. In the SPDIF format, the validity bit V is used as a flag for this purpose. The effect of this is to disable conventional decoders so that no output is produced by the decoder of a conventional receiver. If the data is nevertheless decoded in a standard receiver, the output will comprise white noise.

One operation which may be performed by the unit 42 is to provide on one non-audio channel (e.g. the U channel) a signal which has a transition for each rising edge of the input signal, and to provide on another non-audio channel (e.g. the V channel) a signal which has a transition for each falling edge of the input signal. Of course, numerous other encoding schemes may be employed to enable the random string of data bits to be provided on the non-audio channels in an encoded manner.

The encoding operation described above may be performed purely on the user data stored within the channel frame structure, or may also be performed on the control data of the

channel. Thus, although in Figure 3 the encoder and decoder are shown to operate on the control and user data, the control information may in fact bypass the encoding circuitry, although additional control data is derived from the random number generator. It may be possible for this additional control data may to replace data in the existing defined frame structure. The data and control data may together comprise an I^2S digital audio stream.

The output of the apparatus 18 shown in Figure 4 is provided to a conventional transmitting circuit Tx which reconfigures the data to satisfy the standard interface protocol. Thus, in the example of digital audio data, the encoded data stream DATA', the necessary control data (if not included in DATA') and the additional control signal derived from the random number is formatted into the frame structure illustrated in Figure 2. This data format may be transmitted over a conventional coaxial cable between different pieces of equipment within a data processing apparatus.

As alternatives to the example of a CD player given above, the apparatus 18 may comprise a digital radio, TV or satellite receiver, DVD payer, surround sound decoder, multiroom distribution system or any other signal processing unit. The transmission may be wired or wireless.

Figure 5 shows the architecture of a decoder for receiving the transmitted information and reconstructing the original data.

The decoder 50 essentially comprises units having the inverse functions of the encoder 20 described with reference to Figure 4. Thus, the decoder 50 comprises an inverse transform unit 52 which can recover the random number coded in the control signal, and preferably transmitted over the non-audio channels (in the case of digital audio data transmission). Since this random number is used in the encoding unit to derive the initialization values for the encoding unit 24 in the encoder 20, the same initialization values must be recovered in order to enable the decoding process to function. A transformation unit 54 having the same structure to the unit 34 of the encoder is provided to recover the number α of initialization values used in the encoder at the beginning of each data word. The transformation unit 54 comprises the sequence of latches 56 and the permutation unit 58 corresponding to those units

in the encoder 20. The latches 56 are again triggered by a sample clock SCLK. The clock signals used to control the decoder 50 are recovered from the transmitted data by the receiver Rx in conventional manner. The initialization values which form the output 60 of the inverse transformation unit 54 are supplied to a decoder unit 62 which performs the inverse function to that carried out in the encoder unit 24. For this purpose, a combinatorial unit 64 is provided which enables the original data signal DATA to be reconstructed from a set of decoding bits 66 and the encoded data input 68. In the same way as for the encoding unit 24, the decoding bits 66 are obtained from the output of the inverse transformation unit 54 at the beginning of each word, but are obtained by a feedback path 70 after initialization.

The decoded data output DATA is supplied to a processor 72 which carries out the normal function of the apparatus 48. The apparatus 48 shown in Figure 5 may comprise, as alternatives to the example given above of a loudspeaker, a surround sound decoder, graphic equaliser, multiroom distribution system, D to A converter, power amplifier, video display device, graphics processing device or any other signal processing device receiving a serial digital input.

One particular encoding scheme has been described above in detail, although no details have been given of the exact scrambling functions that may be employed. However, the various possibilities will be apparent to those skilled in the art. Furthermore, the exact number α of bits used as the encoding or decoding bits in the encoding unit 24 or the decoding unit 62 may be any suitable value. A higher number α will enable the whiteness of the encoded data output DATA′ to be increased, but at the expense of greater processing requirements. As one example, number α may equal 16 so that the combinatorial units 26 and 64 perform a transformation function operating on a 17 bit word. The number of bits β of the random word does not need to be the same length so, for example, the transformation unit 38 may convert a 65 bit random word into the series of 16 initialization bits for the encoding unit 24.

The encoding technique described may be implemented in software in a general purpose CPU, in a DSP device, in a gate array IC, in an ASIC, in discrete logic on an a PCB or in some combination of these.

09/913785
531 Rec'd PCT 15 AUG 2001

CLAIMS

1. A data encoding device having a serial data input and an encoded serial data output, wherein the serial input is supplied to an encoding unit which combines each input bit with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and a plurality of updated encoding bits, wherein each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein the combination function performed by the encoding unit combines the input bit with a function of the key, such that over time the encoded output bit stream comprises substantially white noise.

2. A data encoding device as claimed in claim 1, wherein a random number generator is provided which generates a stream of bits, an initial plurality of encoding bits being derived from the output of the random number generator for initialisation of the encoding device.

3. A data encoding device as claimed in claim 2, wherein each random bit is provided to a transformation unit comprising means for storing a predetermined number of previous values of the random bit to derive a multiple bit random word.

4. A data encoding device as claimed in claim 3, wherein the random word is supplied to a permutation unit which generates the initial plurality of encoding bits.

5. A data encoding device as claimed in claim 4, wherein the serial input comprises a string of digital words each comprising a predetermined number of bits, and wherein the random number generator is clocked using a word clock, such that for each digital word of the input a new random bit is generated, and wherein the encoding unit is re-initialized by the output of the permutation unit once for each word.

6. A data encoding device as claimed in claim any preceding claim, wherein the combination performed by the encoding unit is carried out more rapidly than the time associated with the reception of each input bit from the serial data input, such that the encoded

output bit represents the input bit with zero bit delay.

7. A data encoding device as claimed in any preceding claim, wherein the input comprises digital audio data.

8. An apparatus for generating digital audio data comprising a source of digital audio signals, a data encoding device as claimed in any preceding claim, and a transmitter for supplying the encoded serial data output to an output port of the apparatus.

9. An apparatus as claimed in claim 8, wherein the output at the output port is in SPDIF or AES/EBU format.

10. An apparatus as claimed in claim 8 or 9, comprising a compact disc player.

11. A data decoding device for decoding a serial data stream encoded by an encoding device of any one of claims 1 to 7, wherein the stream of input bits is supplied to a decoding unit which combines each encoded input bit with a plurality of additional decoding bits, to extract a decoded output bit and an updated plurality of decoding bits.

12. A data decoding device as claimed in claim 11, wherein a random number extractor is provided for extracting a random number from the input to the decoding device and which provides a plurality of decoding bits for initialisation of the decoding device.

13. An apparatus for reconstructing digital audio signals comprising an input for receiving encoded digital audio signals, a receiver for supplying the encoded digital audio signals to a decoding device as claimed in claim 11 or 12, and an output for the reconstructed digital audio signal.

14. An apparatus as claimed in claim 13, comprising a speaker.

15. A data communications system comprising an apparatus as claimed in claim 8, 9 or 10

for providing an encoded digital audio output, and an apparatus as claimed in claim 13 or 14 for reconstructing the digital audio signal.

16. An apparatus for encoding digital audio signals, the apparatus having an audio input in a format having a dedicated clock signal channel and an encoded audio output in a format having an intrinsically defined clock signal in the output data stream, wherein the audio input is encoded such that the encoded audio output comprises substantially white noise, and the output of the apparatus additionally comprises control data for enabling the audio input to be reconstructed at an associated decoding device.

17. An apparatus as claimed in claim 16, wherein the output format having an intrinsically defined clock signal comprises the SPDIF or AES/EBU data format.

18. An apparatus as claimed in claim 16 or 17, wherein the format having a separate clock channel comprises the I^2C data format.

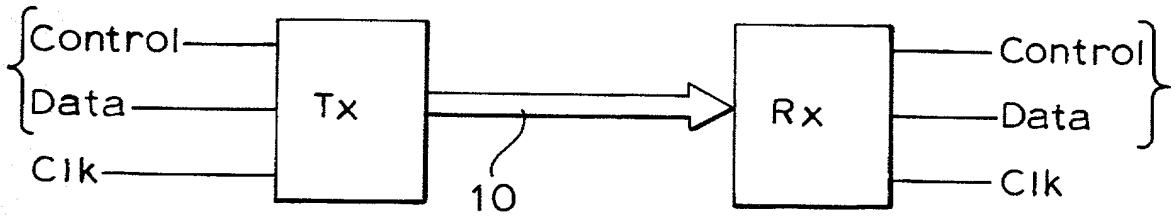


FIG 1

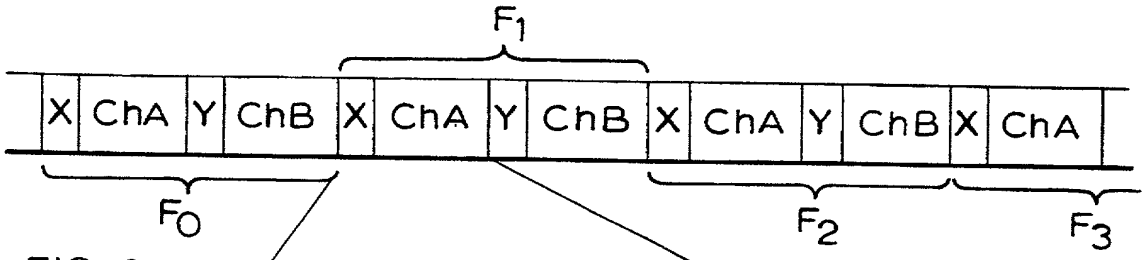
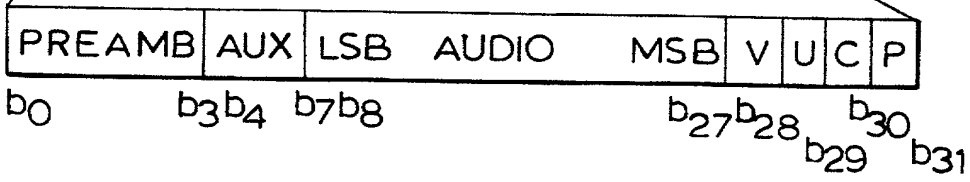


FIG 2



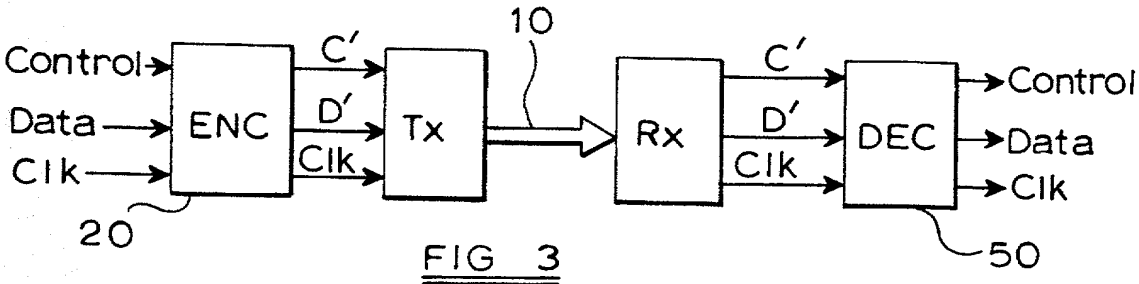


FIG 3

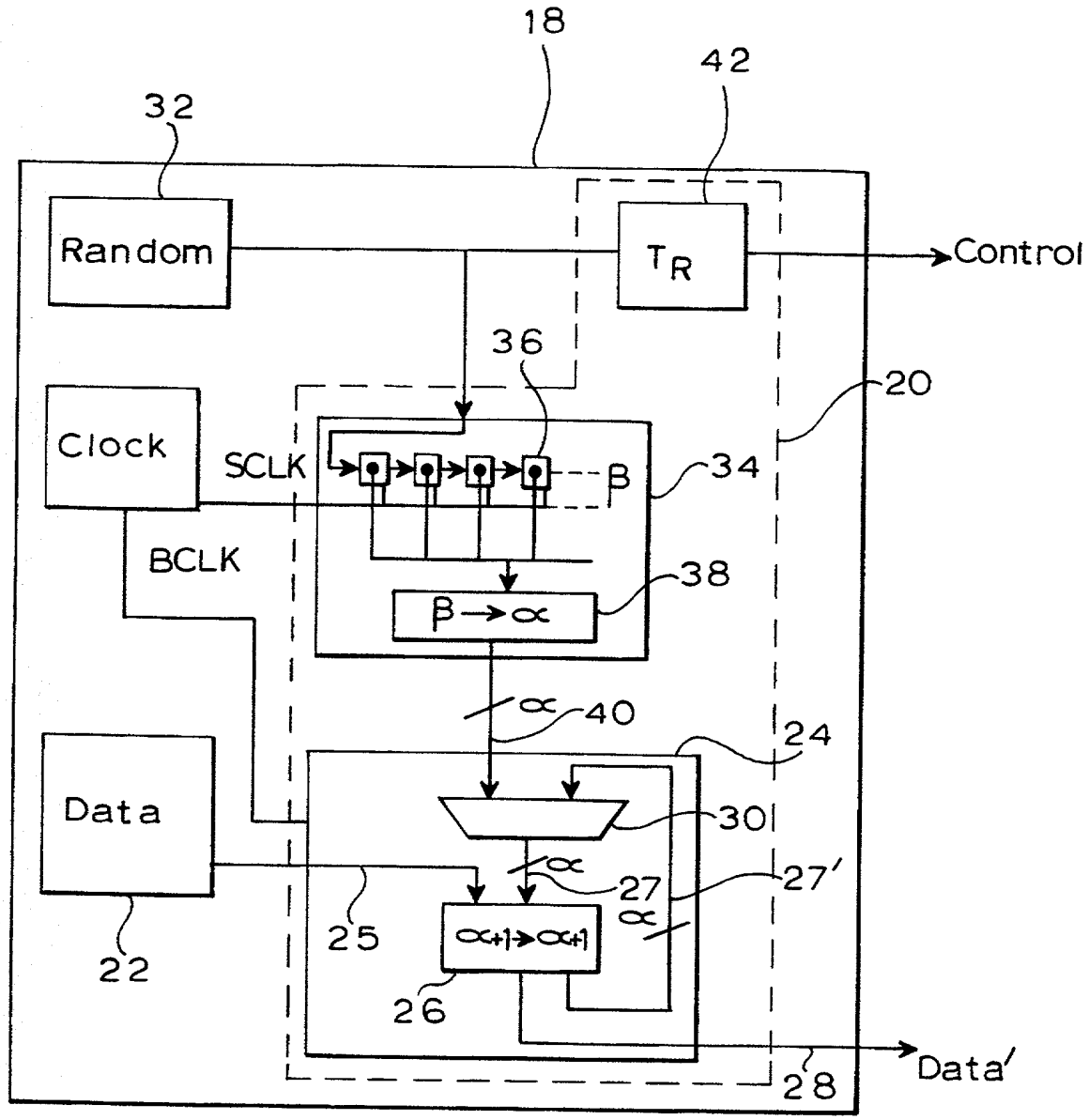

18
42
32
Random
T_R
Control
36
20
Clock
SCLK
β
34
BCLK
38
β→α
α
40
24
Data
30
α
27
27'
α
25
α+1→α+1
22
26
Data'
28

FIG 4

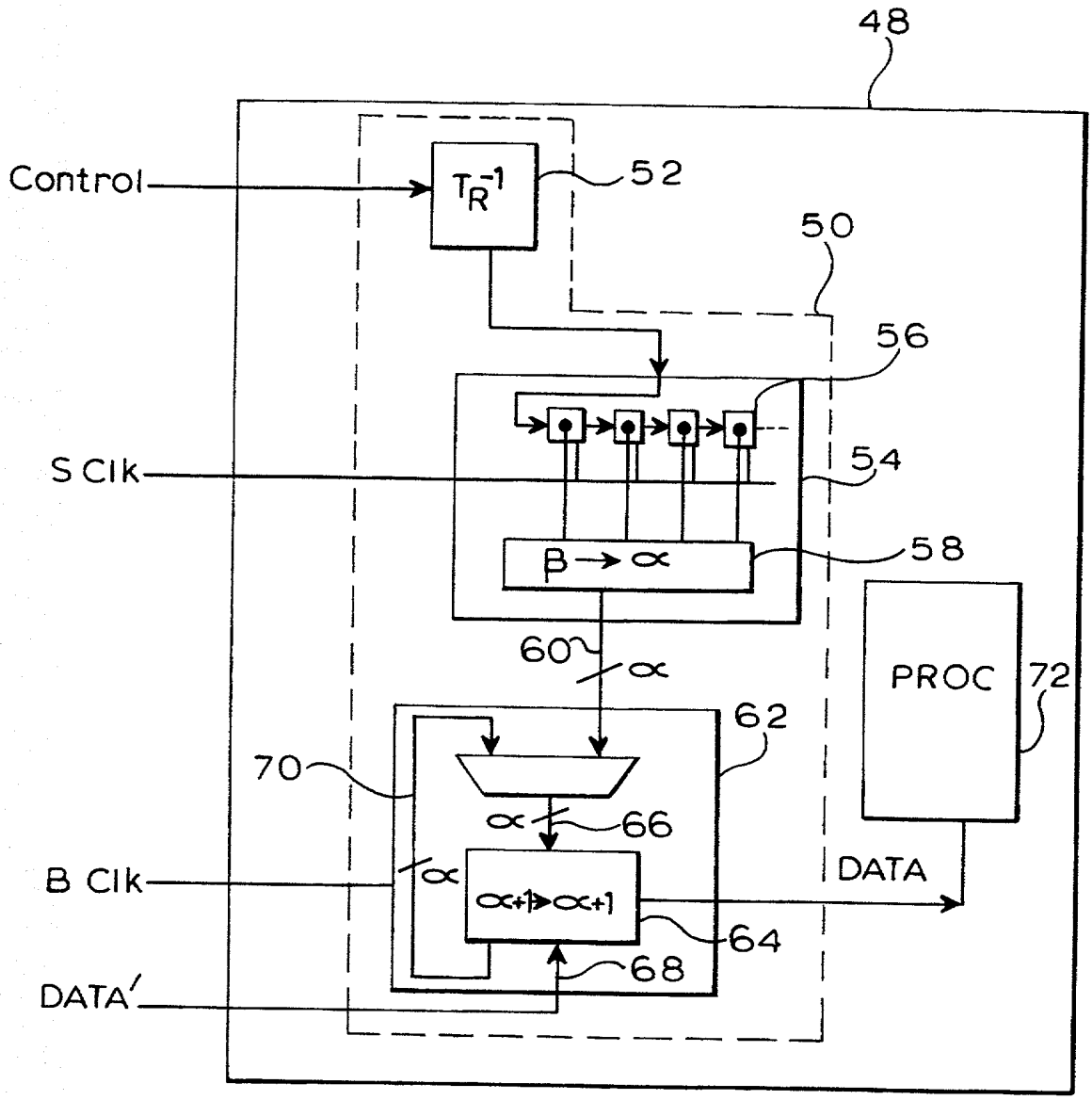

48
Control
T_R^{-1}
52
50
56
S Clk
54
β → α
58
60
α
PROC
72
62
70
α
66
B Clk
α
α+1 → α+1
64
DATA
68
DATA'

FIG 5

JAN 2001

OIPE
JAN 04 2002
PATENT & TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **DATA ENCODING/DECODING DEVICE AND APPARATUS USING THE SAME**, the specification of which:

☐ is attached hereto.

☒ was filed on **11 February 2000** as

Application Serial No. **PCT/GB00/00447**

and was amended on **15 August 2001** if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and

have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

			Priority Claimed	
Country	**Number**	**Date Filed**	**Yes**	**No**
GB	**9903900.0**	**19/02/99**	☒	☐
_____	_____	_____	☐	☐

I hereby claim the benefit under Title 35, United States Code Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

Application Serial No.	Filing Date	Status
_____	_____	_____
_____	_____	_____

And I hereby appoint Thomas E. Smith, Registration No. 18,243, Dennis M. McWilliams, Registration No. 25,195, James R. Sweeney, Registration No. 18,721, William M. Lee, Jr., Registration No. 26,935, Glenn W. Ohlson, Registration No. 28,455, David C. Brezina, Registration No. 34,128, Jeffrey R. Gray, Registration No. 33,391, Timothy J. Engling, Registration No. 39,970, Gregory B. Beggs, Registration No. 19,286, Gerald S. Geren, Registration No. 24,528, Peter J. Shakula,

Registration No. 40,808, and Robert F.I. Conte, Registration No. 20,354, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith. It is requested that all communications be directed to Lee, Mann, Smith, McWilliams, Sweeney & Ohlson, P.O. Box 2786, Chicago, Illinois 60690-2786, telephone number (312) 368-1300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: **Clive JONES**

Signature Clive Jones Date 2001-08-31

Country of Residence: **United Kingdom**

Country of Citizenship: **United Kingdom**

Post Office and Residence Address: **c/o Meridian Audio Ltd**
Stonehill
Stukeley Meadows
Huntingdon
Cambridgeshire PE29 6EX
United Kingdom

GBX

JW

Full name of joint inventor: **Richard HOLLINSHEAD**

Signature R.J. Hollinshead. Date 2 OCTOBER 2001

Country of Residence: **USA**

Country of Citizenship: **United Kingdom**

Post Office and Residence Address: **1066 Honey Creek Road**
Conyers GBX
GA 30013
USA

Full name of joint inventor: _____

Signature _____ Date _____

Country of Residence: _____

Country of Citizenship: _____

Post Office and Residence Address: _____

09/937,985 PCT/GB00/01063